Notice of Allowability	Application No.	Applicant(s)	
	09/707,433	GEIST ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *appeal brief filed on 11/18/2005 and interview conducted on 01/10./06*.

2. ☒ The allowed claim(s) is/are *29, 31-43, 45-61, 63-92, 100-124, 127-138 and 140-144, now re-numbered as claims 1-103*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *enclosed* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ms. Lise A. Rode on 01/10/2006.

The application has been amended as follows:

Claim 29

(Currently amended) A system for creating a [A] self-authenticating document having critical document data, the self-authenticating document comprising:

a first digital signature including a first digest of said critical document data;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored in machine-readable format on said self-authenticating document.

Claim 30

Canceled.

Claim 31

(Currently amended) The self-authenticating document of claim [30]29, wherein said critical document data includes data contained in a magnetic ink character recognition (MICR) code line on said self-authenticating document.

Claim 43

(Currently amended) A system for creating a [A] self-authenticating document having critical document data, the self-authenticating document comprising:

a digital signature including a digest of said critical document data and personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said digital signature, wherein said digital signature and said public key certificate are stored on said self-authenticating document, wherein said public key certificate further includes identity information of the owner of said authentic public key and a digital signature of said authentic public key and said owner identity information, and wherein said digital signature is issued by a third party, and wherein said digital signature and said public key certificate are stored in machine-readable format on said self-authenticating document.

Claim 44

Canceled.

Claim 45

(Currently amended) The self-authenticating document of claim [44] 43, wherein said document is a personal value document.

Claim 51

(Currently amended) The self-authenticating document of claim [44] 43, wherein said machine-readable format is a two-dimensional bar code.

Claim 62

Canceled.

Claim 63

(Currently amended) The self-authenticating document of claim [62]43, wherein said third-party digital signature is created using the elliptic curve digital signature algorithm (ECDSA).

Claim 75

(Currently amended) A system for creating a [A] personal value document, the personal value document comprising:

a first digital signature including a first digest of critical document data, said critical document data including data contained in a magnetic ink character recognition (MICR) code line on said personal value document;

a second digital signature including a second digest of said critical document data and a personal identification number (PIN); and,

a public key certificate including an authentic public key for validating said first and second digital signatures, wherein said first digital signature, said second digital signature, and said public key certificate are stored in a bar code format on said personal value document.

Claim 92

Canceled.

Claim 93

Canceled.

Claim 94

Canceled.

Claim 95

Canceled.

Claim 96

Canceled.

Claim 97

Canceled.

Claim 98

Canceled.

Claim 99

Canceled.

Claim 119

(Currently amended) A method of authenticating a self-authenticating document, comprising the steps of:

processing machine-readable data on said self-authenticating document to obtain digital signature data and a public key certificate;

processing said public key certificate to obtain public key certificate data including an authentic public key and a third-party digital signature, said public key certificate processing step including the substeps of:

validating said public key certificate with a third-party public key by applying said third-party public key to said third-party digital signature; and,

parsing said public key certificate to obtain said authentic public key;

assembling critical document data from said self-authenticating document, wherein said critical document data includes at least magnetic ink character recognition (MICR) data printed on said self-authenticating document;

determining whether an authentic personal identification number (PIN) is available for appending to said critical document data;

wherein, if said authentic PIN is available;

appending said authentic PIN to said critical document data to create an authenticatable data string; and,

applying said authentic public key to said digital signature data to validate said authenticatable data string, wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

Claim 125

Canceled.

Claim 126

Canceled.

Claim 127

(Currently amended) The authenticating method of claim [125]119, wherein said third party is a certificate authority.

Claim 128

(Currently amended) The authenticating method of claim [125]119, wherein said public key certificate is comprised of m bytes, and wherein said public key certificate parsing substep includes the further substeps of:

retrieving at least a first byte, c_1, of said m bytes from said public key certificate, wherein said at least a first byte c_1 is a binary representation of said number of bytes m in said public key certificate;

determining whether said binary representation of said number of bytes m in said at least a first byte c_1, is greater than the number of bytes of data in said digital signature data, n;

retrieving the remainder of said m bytes, if said determining step determines that said at least a first byte c_1 is greater than the number of bytes of data in said digital signature data, n; and,

applying said authentic public key to said digital signature data in order to verify said at least one of said first and second digital signatures.

Claim 135

(Currently amended) A system for reading a self-authenticating document having machine-readable data including critical document data, digital signature data and a public key certificate, the system comprising:

personal identification means for receiving a personal identification number (PIN) from a presenter of said self-authenticating document; and,

image scanning and processing means for reading said self-authenticating document and retrieving said machine-readable data from said self-authenticating document, and for assembling an authenticatable data string from said critical document data and said received PIN;

parsing means for parsing said machine readable data to obtain said digital signature data and said public key certificate; and,

validating means for certifying said public key certificate to obtain an authentic public key, and for applying said authentic public key to said digital signature data for validating said authenticatable data string, said validating means comprising:

a certification validation subsystem for validating said public key certificate with a third party public key and for obtaining said authentic public key; and,

a digital signature validation subsystem for validating said digital signature data with said authentic public key,

wherein said self-authenticating document is authenticated if said authenticatable data string is validated.

Claim 139

Canceled.

2. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
4. Claims 1-28, 30, 44, 62, 93-99, 125, 126 and 139 have been cancelled.
5. Claims 29, 31, 43, 45, 51, 63, 75, 119, 127, 128 and 135 have been amended.
6. Claims 29, 30-43, 45-61, 63-92, 100-124, 127-138 and 140-144, now re-numbered as claims 1-103 are pending.

Response to Arguments

7. Applicant's appeal brief arguments filed 02/11/04 and agreement reached on the interview on 01/10/2006 have been fully considered and they are persuasive.

Allowable Subject Matter

8. Claims 29, 30-43, 45-61, 63-92, 100-124, 127-138 and 140-144 are allowed.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should

preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is 571-272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as 571-272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

01/10/2006

AU 2132